10/500311

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1-18

~~1-19~~ (canceled)

19

~~20~~. (new) A group signature system enabling a member (M) of a group (G) to produce a message (m) accompanied by a signature (S) for proving to a checker (2, 4) that the said message (m) originates from a member (M) of said group (G), using personalized data (z; Kz),

characterized in that said system is electronic and includes an electronic hardware support (26) and in that the said personalized data is integrated into said electronic hardware support (26).

20

~~21~~. (new) A group signature system according to claim 20, characterized in that said hardware support includes encryption means (B3) for personalizing encrypted text (C) using the said personalized data (z; Kz) before the signature (S) of the message (m).

21 20

~~22~~ (new) A group signature system according to claim ~~21~~, characterized in that said hardware support further includes means (B5) for combining the message (m) to be signed and the encrypted text (C) associated with said message (m) in the form of a concatenation of the message (m) with the encrypted text (C).

22

~~23~~. (new) A group signature system according to claim 20, wherein the hardware support further includes signature means (Sig-B6) for producing a signature of the message (m) with the personalized data (z; Kz) in any encrypted form (C) associated with said message.

23
~~24.~~ (new) A group signature system according to claim 21, characterized in the said personalized data is an identifier (z) personal to the member (M), and in that the said electronic hardware support (26) includes an encryption key (K) common to all members of the group (G), and encryption means (B3) for encrypting (C) the identifier (z) with the said encryption key.

24
~~25.~~ (new) A group signature system according to claim 23, characterized in that encryption means (B3) encrypts the text (C) with the identifier (z) and a random number (r).

25
~~26.~~ (new) A group signature system according to claim 21, characterized in that the said personalized data is a diversified encryption key (Kz) specific to each member (M) of the group (G), and in that encryption means (B3) encrypts the text (C) using at least one data (r) with the said encryption key (Kz).

26
~~27.~~ (new) A group signature system according to claim 25, characterized in that the said data (r) includes a random number.

27
~~28.~~ (new) A group signature system according to claim 25, characterized in that the encryption means (B3) uses a secret key encryption algorithm (K).

28
~~29.~~ (new) A group signature system hardware support according to claim 25 wherein the encryption means (B3) use either a public key encryption algorithm RSA (Rivest, Shamir, Adleman) or an AES (Advanced Encryption Standard) public encryption algorithm.

29
~~30.~~ (new) A group signature system according to claim 23, characterized in that the signature means (B6) uses a private key signature algorithm (SK).

30

31. (new) A group signature system according to claim 30, characterized in that the private key signature algorithm is of the RSA type (Rivest, Shamir, Adleman).

31

32. (new) A group signature system according to claim 20, characterized in that said hardware support comprises a portable communicating device (26).

32

33. (new) A group signature system according to claim 32, characterized in that said portable communicating device is a smart card (26).

33

34. (new) A method for checking a message (m) sent by a member (M) of a group (G) accompanied by a signature (S) wherein the message (m) authentication the signature to indicated that the message originates from a member of the group, comprises producing the signature (S) of the message (m) with a private key (SK) common to members (M) of the group (G) and integrating personalized data (z; KZ) electronic hardware support (26) into the message, transmitting the message with the authenticated signature to a user of the system (2,6) without needing to supply proof to the user that the member (M) belongs to the said group (G).

34

35. (new) A method for checking a message (m) sent according to claim 34, characterized in that the message is checked using a public key corresponding to the said private key (SK).

35

36. (new) A method for opening a signature (S) produced by a group signature system which enables a member (M) of a group (G) to produce a message (m) accompanied by the signature (S) so as to authenticate the signature (S) for a user of the system comprising the steps of:

making correspondence data between the identities of members (M) of the group (G) and their personalized data available, before the signature;

decrypting the personalized data received from an electronic hardware support (26) for which the signature is to be opened; and

opening the signature when the decrypted personalized data corresponds to the identity of the member (M) of the group (G).

36

37. (new) A method for adapting an electronic hardware support (26) for a group signature system which enables a member (M) of a group (G) to produce a message (m) accompanied by a signature (S) to authenticate the signature (S) for a user of the system wherein the hardware support is personalized to a member (M) of the group, characterized in that it comprises steps consisting of:

producing personalized data (z; Kz) to be used for the said electronic hardware support (26) to be personalized; and

registering this personalized data with a private signature key (SK) in the said hardware support.

37

38. (new) A group signature system, comprising a terminal (10), said terminal including means for reading a portable communicating device issued to a member (M) of a group by a trusted authority, said device being personalized to the member (M) with personalized data integrated into the device in the form of an identifier (z, Kz) so as to be capable of producing a message and signature associated with the group;

said device including encryption means for making a personalized encrypted text using the personalized data before the signature of the message and means for making a combination of the message to be signed and the encrypted text

associated with the message in the form of a concatenation of the message and the encrypted text.

38

39. (new) A group signature system as set forth in claim 38 wherein said device further includes means for producing the signature associated with the message in encrypted form using the personalized data and wherein users within the system include commercial entities which require a signature to be authenticated.